

REMARKS

Claims 16-39 remain in the application, with claims 16 and 28 in independent form. Claims 1-15 have been previously canceled.

The claims have been carefully reviewed with particular attention to the points raised in the Office Action. It is submitted that no new matter has been added and no new issues have been raised by the present response.

Independent claims 16 and 39 were rejected under 35 U.S.C. § 103(a), as allegedly being unpatentable over the document by Burrows ("A Logic of Authentication"). Applicants are uncertain whether this document was ever published and, therefore, whether it constitutes prior art. Applicants will herein distinguish the document's disclosure without conceding that the document is prior art.

Independent claim 16 relates to a method for mutual authentication of a terminal and a network. A triplet data set is received at the network from an authentication center. The triplet data set includes a first random number (challenge 1), a first response (response 1) and a second response (response 2). The first random number (challenge 1) is sent to the terminal. A first calculated response, sent by the terminal, is received. The first calculated response is calculated by the terminal based on the first random number (challenge 1). The first calculated response is used as a

second challenge (challenge 2). The terminal is authenticated by matching the first calculated response with the first response (response 1). The second response (response 2) is sent to the terminal. The network is authenticated by the terminal by matching a second calculated response, calculated by the terminal based on the first random number (challenge 1) with the second response (response 2).

In claim 16, an authentication procedure is carried out between two entities M and N where an Authentication Center Auc delivers authentication data to N. The Auc delivers a first random number (challenge 1), a first response (response 1) and a second response (response 2) to N.

The cited portions of Burrows relate to an explanation of the Needham-Schroeder Protocol (with shared keys) for authenticating two entities A and B and a server S, where S delivers authentication data to A.

It can be implied from the Office Action that the Examiner maintains that the entity "A" of Burrows corresponds to the entity "N" of claim 16, the entity "B" of Burrows corresponds to the entity "M" of claim 16, and that the server "S" of Burrows corresponds with the Auc of claim 16.

The Examiner also implies that $\{K_{AB}, A\}_{K_{BS}}$ corresponds to Challenge 1, K_{AB} corresponds to Response 1, and N_A corresponds to Response 2.

Put simply, the Examiner has laid out the following

comparison:

A corresponds to N
 B corresponds to M
 S corresponds to Auc

$\{K_{AB}, A\}K_{BS}$	corresponds to	Challenge 1
K_{AB}	corresponds to	Response 1
N_A	corresponds to	Response 2

Using the Examiner's analysis above, a detailed comparison between the technique of Burrows and claim 16 reveals that the two techniques are not the same and that the technique of Burrows fails to teach or suggest the content of claim 16.

The table below is provided to help illustrate the correspondences between claim 16 and Burrows so that proper attention may be drawn to their differences.

Message	Claim 16	Needham-Schroeder Protocol (Burrows)
1. $A \rightarrow S$	Triplet Request	A, B, N_A
2. $S \rightarrow A$	Challenge 1, Response 1, Response 2	$\{N_A, B, K_{AB}, \{K_{AB}, A\}K_{BS}\}K_{AS}$
	Challenge 1, Response 1, Response 2	$\{K_{AB}, A\}K_{BS}$ K_{AB} N_A
3. $A \rightarrow B$	Challenge 1	$\{K_{AB}, A\}K_{BS}$
4. $B \rightarrow A$	Response 1 = Challenge 2	$\{N_B\} K_{AB} \neq K_{AB}$
5. $A \rightarrow B$	Response 2	$\{N_B - 1\} K_{AB} \neq N_A$

In the table above, the 5 messages of Burrows taken from page 18 are overlaid with the comparable steps taken from claim 16. It can be seen that steps 4 and 5 of Burrows differ from the corresponding steps of claim 16 because in message 4,

Burrows transmits $\{N_B\}K_{AB}$ while claim 16 uses Response 1 which is assumed to correspond to K_{AB} . Additionally, in message 5, Burrows transmits $\{N_B - 1\}K_{AB}$ while claim 16 uses Response 2 which is assumed to correspond to N_A .

A similar comparison reveals that Burrows does not teach or suggest the method of independent claim 28:

Message	Claim 28	Needham-Schroeder Protocol (Burrows)
1. $A \rightarrow S$	Triplet Request	A, B, N_A
2. $S \rightarrow A$	Challenge 1, Response 1, Response 2	$\{N_A, B, K_{AB}, \{K_{AB}, A\}K_{BS}\}K_{AS}$
	Challenge 1, Response 1, Response 2	$\{K_{AB}, A\}K_{BS}$ K_{AB} N_A
3. $A \rightarrow B$	Challenge 1 Response 2	$\{K_{AB}, A\}K_{BS}$ No Response $\neq N_A$
4. $B \rightarrow A$	Response 1 = Challenge 2	$\{N_B\} K_{AB}$ $\neq K_{AB}$

In the table above, the messages of Burrows taken from page 18 are overlaid with the comparable steps taken from claim 28. It can be seen that steps 3 and 4 of Burrows differ from the corresponding steps of claim 28 because in message 3, Burrows fails to transmit N_A which is assumed to correspond with Response 2. Additionally, in message 4, Burrows transmits $\{N_B\}K_{AB}$ while claim 28 uses Response 1=Challenge 2, which is assumed to correspond to K_{AB} .

Accordingly, independent claims 16 and 28 are patentably distinct from the cited art for at least the above-stated reasons. Moreover, dependent claims 17-27 and 29-39 are patentably distinct from the cited art for at least similar

reasons.

The Office is hereby authorized to charge any fees which may be required in connection with this amendment and to credit any overpayment to Deposit Account No. 03-3125.

Favorable reconsideration is earnestly solicited.

Respectfully Submitted,

Dated:

1-24-06

Norman H. Zivin

I hereby certify that this paper is being deposited this date with the U.S. Postal Service as first class mail addressed to:
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Norman H. Zivin 1-24-06
Reg. No. 25,385 Date

Norman H. Zivin
Registration No. 25,385
c/o Cooper & Dunham LLP
1185 Avenue of the Americas
New York, New York 10036
(212) 278-0400
Attorney for Applicants